Department of Homeland Security Daily Open Source Infrastructure Report for 15 May 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Baltimore's Mercantile Bankshares Corp. reported on Friday, May 12, that a laptop computer containing Social Security and account numbers for nearly 50,000 customers of its Bethesda−based Mercantile Potomac Bank was stolen a week earlier from a worker's car off company property. (See item 12)
- The North American Aerospace Defense Command will be monitoring waterways around North America as part of a revised defense agreement that contains no expiration date between Canada and the United States. (See item 18)
- The Transportation Security Administration and the U.S. Coast Guard on Wednesday, May 10, took another step toward the implementation of the Transportation Worker Identification Credential by approving proposed regulations for a biometric−based identification credential for port workers. (See item 22)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *May 12, New York Times* — **Up to 200 people die in Nigeria oil blast.** Some 150 to 200 people were burned to death Friday, May 12, when a fuel pipeline exploded about 30 miles east

of Nigeria's principal city of Lagos. The cause was the result of vandals who damaged the pipeline in an effort to steal gasoline for personal use or to re−sell in other locations, officials said, rather than the work of political rebels who are active in the southern part of the country. Officials said many of the victims were local residents who rushed to collect fuel spilling out of the pipeline, an action known as "scooping." The pipe had been dug out of the sand and bore visible marks of drilling, they said. Some 500 cans designed to hold gasoline were found nearby and apparently contributed to the fire once it was ignited. Stealing fuel or crude oil from pipelines is common in Nigeria, one of the world's largest oil producers, despite the obvious dangers. The pipeline that exploded Friday belongs to a state−owned company, the Nigerian National Petroleum Corporation, and was buried just under the surface of a sandy beach on one of the many islands near Lagos.
Source: http://www.nytimes.com/2006/05/12/world/africa/12cnd−nigeria .html?hp&ex=1147492800&en=b583475ddd9e2caa&ei=5094&partner=h omepage

2. *May 12, Reuters* — **Blast hits Gary−Williams refinery.** An explosion rocked the 53,000−barrel per day (bpd) Gary−Williams Energy Corp. refinery in Wynnewood, OK, on Friday, May 12, the company said. No deaths or injuries were reported. There were no indications of sabotage on Friday afternoon. The explosion occurred in an alkylation unit at the refinery at about 2 p.m. CDT, said Sally Allen, vice president of administration and governmental affairs. Allen said she did not if all operations at the refinery were halted due to the explosion and fire. The refinery in Wynnewood, 67 miles south of Oklahoma City, is operated by Wynnewood Refining Co. The refinery produces gasoline, diesel fuel, military jet fuel, solvents, and asphalt.
Source: http://today.reuters.com/news/newsArticle.aspx?type=domestic News&storyID=2006−05−12T234340Z_01_N12444389_RTRUKOC_0_US−EN ERGY−WYNNEWOOD−REFINERY.xml&archived=False

3. *May 11, Tribune (CA)* — **NRC: 2005 Diablo plane incident unlikely.** A Nuclear Regulatory Commission (NRC) investigator has determined that a report of a private airplane diving toward Diablo Canyon nuclear power plant a year ago is probably untrue. San Luis Obispo Mothers for Peace activist Jane Swanson made the allegation at an NRC public hearing in San Luis Obispo after she received an anonymous call from a man who claimed to be riding in a private plane May 14 or 15 last year when the pilot made a steep dive on the power plant, which is located in San Luis Obispo County, passing 500 feet over the containment domes. Pacific Gas and Electric Co. (PG&E) officials discounted the allegation because no one at the plant observed the incident. "It would have been impossible for that incident to have occurred as described without us knowing about it," said Jeff Lewis, plant spokesperson. The NRC referred the incident to PG&E for further investigation and concurred with the utility's finding that it is unlikely a dramatic incident such as a plane swooping down on the plant would have gone unnoticed.
NRC Report: http://www.sanluisobispo.com/multimedia/sanluisobispo/archiv e/diablodiver.pdf
Source: http://www.sanluisobispo.com/mld/sanluisobispo/14551669.htm

4. *May 11, Toronto Star (Canada)* — **Backup power eyed for peaks.** During the 2003 blackout, hundreds of highrise buildings, companies, hospitals, and other organizations across Ontario kept the lights on by firing up their own emergency diesel generators. But why wait for a blackout? Toronto Hydro Corp., as part of its "PeakSaver" program, plans to demonstrate how

backup generators can play a role in meeting the city's power demands, especially during the hottest summer days when the province is forced to import expensive and often dirty electricity. By remotely activating backup generators at the Air Canada Center, North York General Hospital, First Canadian Place, and a number of other large commercial buildings, the utility hopes to displace up to ten megawatts of grid electricity. Toronto Hydro spokesperson Tanya Bruckmueller−Wilson said the voluntary program is expected to attract enough commercial participants for the utility to displace, when needed, up to 130 megawatts (MW) of grid power by the end of next year. This is on top of 70 MW that the program aims to save by tapping into and, with permission, turning down residential and business air conditioning systems when the grid is most strained.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1147297812711&call_pageid=968350072197&col=969048863851

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *May 12, WTHR (IN)* — **Chemical spill prompts road closure; residents asked to remain indoors.** About 20 gallons of sulfuric acid were spilled inside the Magnode Corp. aluminum finishing plant in Indianapolis, IN, Friday, May 12. As firefighters neutralized the chemical, residents in the area were asked to stay indoors. In addition, West Washington Street was closed due to the spill.
Source: http://www.wthr.com/Global/story.asp?S=4896310&nav=9Tai

6. *May 12, WZZM 13 (MI)* — **Kerosene leaks into Michigan sanitary sewer system.** Over 1,000 gallons of kerosene from a phone company in Grand Haven, MI, leaked into the sanitary sewer system, prompting closure of Washington Avenue. The exact amount of kerosene that leaked into the system remains undetermined. Personnel from the Ottawa County Hazmat team, U.S. Coast Guard Grand Haven Station, and the U.S. Army Corps of Engineers were called out to boom the river to help prevent the kerosene from being discharged into the Grand River.
Source: http://www.wzzm13.com/news/news_article.aspx?storyid=54331

[Return to top]

Defense Industrial Base Sector

7. *May 11, Air Force Link* — **Smart Operations 21 office formed at Pentagon.** In February, Air Force leaders created a new program office at the Pentagon that will take the lead in optimizing the way the Air Force conducts its mission. The Air Force Smart Operations 21 office, created in response to an initiative by Secretary of the Air Force Michael W. Wynne, will look at process improvement across the service. The new office provides top−level guidance for implementing AFSO21 initiatives. These initiatives will enhance a mindset in the Air Force that is already geared toward innovation, said Brig. Gen. S. Taco Gilbert III, director of the Air Force Smart Operations 21 office. "The Air Force has always fostered a culture of innovation," General Gilbert said. "We are trying to take that culture of innovation to the next level, where

we look at all the processes involved in what we do. We look at not doing 'more with less,' but at being smarter about the way we are doing business −− eliminating work that is unnecessary." Senior leaders designed the program specifically for the Air Force, and it is based on similar industry process improvement practices like Lean, Six Sigma and Theory of Constraints.
Source: http://www.af.mil/news/story.asp?id=123020236

8. *May 11, U.S. Department of State* — **U.S. seeks to expand umbrella of missile defense coverage.** The director of the U.S. Missile Defense Agency says robust defenses are needed against a broad range of current and evolving strategic and tactical ballistic missile threats. Air Force Lieutenant General Henry "Trey" Obering told members of Congress Wednesday, May 10, that the U.S. and key partners are working to expand the existing umbrella of defensive coverage to prevent the U.S. and its allies from being coerced or threatened by ballistic missiles −− possibly carrying a weapon of mass destruction. Lieutenant General Larry Dodgen, who leads the Army's Space and Missile Command and testified at the hearing alongside Obering, also pointed to increased interest in missile defense within the North Atlantic Treaty Organization (NATO). NATO has been studying missile defense requirements, he said, and is expected to "come forward next year with some recommendations as to what they want to field."
Source: http://usinfo.state.gov/xarchives/display.html?p=washfile−english&y=2006&m=May&x=20060511162234sjhtrop0.3299066&t=livefe eds/wf−latest.html

9. *May 11, Defense News* — **U.S.−India deal: No favors for U.S. defense firms, official says.** The U.S. is seeking no preferential treatment from India for the American defense industry in the countries' proposed nuclear cooperation deal, a senior U.S. Department of State official said. The U.S. industry "competes well on a level playing field in defense or other areas," said Philip Zelikow, senior policy adviser to Secretary of State Condoleezza Rice. India's military has plans to buy weapons and equipment worth several billion dollars. The biggest is the $8.5 billion effort to buy 200 fighter jets for the air force's Multi−role Combat Aircraft program. The U.S. Lockheed Martin F−16 and Boeing F/A−18 are competing against the Russian MiG, Swedish Gripen and French Mirage fighter jets. India has traditionally purchased Russian and European weapons.
Source: http://www.defensenews.com/story.php?F=1768629&C=america

[Return to top]

Banking and Finance Sector

10. *May 15, Dayton Daily News (OH)* — **Colleges boost computer security as hackers persist.** Local college officials say they were beefing up computer security before the most recent data breaches at Ohio University (OU) and the University of Texas (UT) −− but those cases show the importance of daily vigilance. Prior to the two breaches, the University of Dayton hired an information technology risk management officer and brought in an outside company to perform a complete security audit, said Thomas Skill, the University of Dayton's chief information officer. The university keeps student data by student ID numbers rather than Social Security numbers, and has combed through its databases to ensure it is not keeping personal data in computer systems unless absolutely necessary. Wright State University (WSU) uses proven data−theft prevention techniques including encryption, firewalls, and other methods, and

reassesses and tightens its security measures on a daily basis, said Patricia Vendt, WSU's information security officer. The OU and UT cases show that identity theft "is here to stay, and we are going to have to do everything we can to protect our data," Vendt said. Miami University has four people in its information security office and upgraded its hardware and installed a stronger firewall last spring, a Miami spokesperson said.
Source: http://www.daytondailynews.com/localnews/content/localnews/daily/0511datatheft.html

11. *May 13, Daytona Beach News Online (FL)* — **Suspicious pipe sparks scare at Edgewater bank.** A morning bomb scare shut down an Edgewater, FL, bank for a few hours and part of State Road 442 for about 40 minutes Friday, May 12. The object was found in the front parking lot of Wachovia Bank, 1813 S. Ridgewood Ave., about 9 a.m. EST. Bank customers and employees were evacuated. The Volusia County Bomb Squad detonated the suspicious object −− a copper tube about five inches long. Both ends of the tube were capped, giving it the appearance of a pipe bomb, said Edgewater Deputy Chief John Taves. The remnants will be sent to the Florida Department of Law Enforcement lab to determine if it was an explosive device, Taves said.
Source: http://www.news−journalonline.com/NewsJournalOnline/News/EastVolusia/evlEAST03051306.htm

12. *May 13, Baltimore Sun* — **Stolen laptop had bank data of 50,000.** Baltimore's Mercantile Bankshares Corp. reported on Friday, May 12, that a laptop computer containing Social Security and account numbers for nearly 50,000 customers of its Bethesda−based Mercantile Potomac Bank was stolen a week earlier from a worker's car off company property. None of the Mercantile Potomac customers has reported suspicious activity, but the bank is offering affected clients one year of a credit−monitoring service. Stephen K. Heine, senior vice president of Mercantile's client service group, said the employee violated bank policy by taking the laptop out of the office his car was broken into. Mercantile did not identify the employee and would not say what disciplinary action, if any, was taken.
Source: http://www.tmcnet.com/usubmit/2006/05/13/1648739.htm

13. *May 13, Charlotte Observer (NC)* — **Man guilty of bank heist plan intended to use explosives to throw off security.** A Charlotte, NC, man has been convicted of concocting a brazen plan to rob a Bank of America branch in Founders Hall. His plan included throwing Molotov cocktails into a branch across Tryon Street to cause a distraction. Munoz−Mendez was arrested November 17, the day before he planned to rob the bank, U.S. Attorney Kevin Zolot said. An undercover FBI agent met Munoz−Mendez and got him to detail his plan for the robbery. The agent said that Munoz−Mendez asked him to throw a bomb into the branch across the street at 4:30 p.m. EST, November 18. He said the distraction would send police and security to the branch, and then he would rob the smaller branch inside Founders Hall. If they resisted, he said, he would shoot security guards to wound but not kill them. He planned to go into the vault and teller drawers, expecting to get $100,000, Zolot said. Zolot said witnesses testified that Munoz−Mendez drew a diagram and walked the route with the undercover officer. The FBI agent videotaped Munoz−Mendez in a field making Molotov cocktails out of kerosene, malt liquor bottles, and T−shirts.
Source: http://www.bradenton.com/mld/charlotte/news/14570015.htm

14. *May 12, Fox 12 (OR)* — **Security breach could now affect more bank customers.** New information about a security breach that looked to affect customers with debit cards ending in the numbers 3100, reveals that customers with card numbers ending in 3100, and 6826, 7200, 6118, 4403, and 4559 may also be affected. Customers in possession of these cards are getting letters from Bank of America (B of A) telling them their check card account information may have been compromised at a third party location. B of A officials will not say who the third party is. Banking experts say it could be related to an overseas scam that happened several months ago when someone used an Office Max computer to access 200,000 accounts. B of A officials say there's no evidence thieves have drained anyone's accounts.
Source: http://www.kptv.com/Global/story.asp?S=4889370

15. *May 11, Register (UK)* — **Foreign ATM fraud loophole exposed by crooks.** Lloyds TSB has admitted that flaws in the new Chip and PIN system recently introduced for debit cards in the UK open up the system to fraud. Although cloned cards won't have a forged chip, the PIN associated with this microchip is the same as that associated with a magnetic stripe. Foreign ATMs only read this magnetic strip and not the PIN. So providing scammers obtain the data on the magnetic strip, along with the associated PIN, they are able to make withdrawals overseas using a conventionally cloned card, something that wouldn't work on a UK high street. Delays in identifying foreign ATM cash withdrawals as potentially fraudulent are compounding the problem. One Lloyds TSB customer had thousands of dollars withdrawn from an account via a series of 19 withdrawals in the Netherlands. Similar scams involving cash machines in France, Thailand, and Hong Kong have hit other customers.
Source: http://www.channelregister.co.uk/2006/05/11/lloyds_tsb_chip_and_pin_fraud/

16. *May 11, SC Magazine (UK)* — **FTC launches identity theft campaign.** The Federal Trade Commission (FTC) has launched an identity theft education campaign to coincide with President Bush's creation of a task force designed to tackle America's fastest growing crime. The FTC's "AvoID Theft: Deter, Detect, Defend" program plans to send 4,500 education kits to victim advocacy groups across the nation, the agency said. Materials include a victim recovery guide, training booklet and 10−minute video on ID theft. "Personal information is the new currency...Consumers should protect their personal information as carefully as they protect their cash," FTC Chairperson Deborah Platt Majoras said. Coinciding with the campaign is the creation of a new federal task force made up of representatives from 13 government agencies. "This task force should help improve coordination among federal, state and local authorities," said Bill Conner, president and CEO of Entrust.
Source: http://www.scmagazine.com/uk/news/article/558745/ftc+launches+id+theft+prevention+program/

[Return to top]

Transportation and Border Security Sector

17. *May 12, Associated Press* — **Delta Air Lines reports first−quarter loss.** Delta, the nation's third−largest carrier, reported on Thursday, May 11, a first−quarter loss of $2.1 billion, plunging the beleaguered airline into deeper financial straits. Excluding a flurry of bankruptcy restructuring costs, however, the Atlanta−based airline's losses are a tamer $356 million for the January to March period. Another example of the company's staggering restructuring costs: It

said it will post a $1.6 billion loss during March alone, but all but $6 million of those losses are from restructuring fees and one−time charges. Yet the massive one−time costs −− including this quarter's $1.4 billion charge to rework financing agreements for a fleet of aircraft and $310 million in accounting adjustments −− still add up to red ink for the airline. Delta has lost more than $14 billion since January 2001. The airline continues trying to emerge from bankruptcy protection it filed for in New York last September.
Source: http://www.usatoday.com/travel/flights/2006−05−12−delta−ap_x .htm

18. *May 12, Colorado Springs Gazette* — **NORAD takes on maritime monitoring.** Monitoring of waterways around North America is now part of a revised defense agreement between Canada and the United States. The agreement's five−year extension, which expired on Friday, May 12, has been replaced with an updated version that contains no expiration date for the first time since Canada and the United States launched the North American Aerospace Defense Command (NORAD) in 1958. "The new agreement is of indefinite duration, acknowledging the mature nature of the United States and Canada defense partnership and the only bi−national command the United States has with any country," said Department of State spokesperson Joanne Moore. The 10th and latest renewal, the first since the September 11, 2001, attacks, is noteworthy because of the addition of maritime monitoring. NORAD, based at Peterson Air Force Base, was formed during the Cold War and monitors air and space threats from inside and outside North America.
Source: http://ebird.afis.mil/ebfiles/e20060512434219.html

19. *May 12, Reuters* — **Indian airports to mount vigil against 'human bomb' threat.** A "human bomb" could attempt to hijack a plane in India, intelligence agencies have warned, prompting security forces to seek state−of−the−art body scanners, an official said on May 12. Intelligence agencies had also warned that airports and dockyards were "targets number one" for militants, especially Islamist militants fighting Indian rule in the restive Himalayan state of Kashmir. The Central Industrial Security Force (CISF, which protects 54 of India's main airports, has asked the government to allow installation of human body scanners at 16 airports in the country categorized as "hypersensitive." These scanners use advanced X−Ray technology to draw a skeletal image of a human body and are considered to be a "fool−proof" measure against hijacking. Earlier this week, police said three suspected Islamist militants arrested in western India with a huge cache of weapons and explosives were planning to attack the Kandla Port, India's largest. The use of body scanners has come in for some criticism in the West as passengers have complained that it amounts to a strip−search and violates their privacy.
Source: http://www.defensenews.com/story.php?F=1770172&C=airwar

20. *May 11, Associated Press* — **Worcester officials vote to add 'Boston' to airport name.** The Airport Commission at Worcester Regional Airport has unanimously recommended the airfield change its name to Worcester−Metrowest−Boston Airport to increase its visibility. Last month, Manchester Airport in Manchester, NH, changed its name to Manchester−Boston Regional Airport for the same reason. Worcester is about 45 miles from Boston, while Manchester is about 50 miles away. The recommended name change for Worcester was part of a consultant's report released last year that offered suggestions on how the struggling airfield could draw more travelers.
Source: http://www.usatoday.com/travel/flights/2006−05−11−worcester− boston_x.htm

21. *May 11, Associated Press* — **Thunderstorms could delay air travel.** The number of airline flight delays in April was 31 percent higher than the same month last year, thanks mostly to a thunderstorm pattern that could mean trouble ahead for summer travelers, the head of the Federal Aviation Administration (FAA) said Thursday, May 11. The severe storms typical of summer arrived earlier this year and with greater frequency, said Marion Blakey. "That doesn't bode well" for the coming months," she said. At the 35 busiest airports, through which almost all passengers travel, the number of delays rose to 922 in April from 704 during the same month last year. The sheer number of travelers will make it harder to deal with delays and cancellations, Blakey said, because airlines have fewer empty seats in which to put stranded travelers. For the past two years, the FAA has monitored delays closely from its Air Traffic Control System Command Center in Herndon, VA, keeping planes on the ground at smaller airports so large airports can clear away backed−up traffic. The result is more and smaller delays, but the aviation system as a whole functions better, Blakey said.
Source: http://www.usatoday.com/travel/flights/2006−05−12−storms−sum mer−travel_x.htm

22. *May 10, Transportation Security Administration* — **Department of Homeland Security issues proposed Rulemakings for Transportation Worker Identification Credential.** The Transportation Security Administration (TSA) and the U.S. Coast Guard on Wednesday, May 10, took another step toward the implementation of the Transportation Worker Identification Credential (TWIC) by approving proposed regulations for a biometric−based identification credential for port workers. The notice of proposed rulemaking will be published in the Federal Register in the coming days and lays out specific details on the program. The public will have forty−five days to comment and four public meetings will be hosted by TSA and Coast Guard to solicit public input. “TWIC is designed to ensure that individuals posing a security threat do not gain access to our nation’s ports,” said Assistant Secretary Kip Hawley of TSA. “Today’s proposed rulemaking represents a significant milestone towards putting TWIC on the fast track.” Also on Wednesday, the Coast Guard approved a proposed regulation that works in conjunction with TWIC to streamline the current credentialing process for merchant mariners. TSA laid the foundation for the establishment of the universal credential through a technology evaluation and prototype test. During the prototype test of the credential last year, TSA issued more than 4,000 TWICs to workers at 26 sites in six states.
TWIC Implementation in the Maritime Sector:
http://www.tsa.gov/public/interweb/assetlibrary/1652_AA41NPR MTWIC_FINAL51006.pdf
Source: http://www.tsa.gov/public/display?theme=40&content=090005198 01db7db

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

23. *May 13, Associated Press* — **Japan confirms mad cow case.** Japan has confirmed its 26th case of mad cow disease, this one in a five−year−old Holstein in the country's north, the Agriculture

Ministry said Saturday, May 13. Meat inspectors in the northern state of Hokkaido found Thursday, May 11, that a dairy cow tested positive for the disease, the ministry said in a statement. A panel of Agriculture Ministry experts confirmed the infection Saturday, May 13, according to ministry official Akiko Suzuki.
Source: http://www.signonsandiego.com/news/world/20060513−0022−japan −madcow.html

24. *May 13, Agence France−Presse* — **Austria confirms fourth case of mad cow disease.** Austria has confirmed it has found a fourth case of mad cow disease, this time in the northern province of Upper Austria, Health Minister Maria Rauch−Kallat said. The Agency for Health and Food Safety confirmed a six−year−old cow at a slaughterhouse in the provincial capital of Linz tested positive for bovine spongiform encephalopathy. The cow came from a farm in the Muehlviertel region, bordering Germany and the Czech Republic. All cattle from the farm have already been slaughtered and the farm and slaughterhouse have been closed and disinfected, the Austria Press Agency reported Saturday, May 13.
Source: http://news.yahoo.com/s/afp/20060513/hl_afp/austriahealthmad cow_060513181248

25. *May 12, USAgNet* — **Africa aims to control animal diseases.** A new initiative has been launched to promote animal health activities in Africa. The move follows a meeting in Bamako, Mali, held in April 2006 between representatives of the World Organization for Animal Health, the Food and Agriculture Organization (FAO), and the Inter−African Bureau for Animal Resources of the African Union. The African Livestock Platform, managed by the World Bank, together with the World Organization for Animal Health, FAO, African Union Inter−Bureau for Animal Resources, and all African institutions involved in the control of animal diseases, have been identified by donors as an optimal coordination mechanism in order to promote animal health and production in Africa as well as to participate as a key player in the prevention and control of avian influenza. Regional Animal Health Centers have been created to implement new programs aimed at improving animal health in Africa and in particular at strengthening the control of Avian Influenza.
Source: http://www.usagnet.com/story−national.cfm?Id=889&yr=2006

26. *May 12, Washington Post* — **Rockfish data to be pooled.** Scientists studying a wasting disease that infects rockfish in the Chesapeake Bay agreed to coordinate their research better to determine what causes the disease and how extensive it is in the striped bass population, researchers said Thursday, May 11, after a two−day conference. Comparing notes at the conference in Annapolis, MD, scientists from more than a dozen state and federal agencies and research groups found that some research on mycobacteriosis conflicted, was repetitious or was stated in a way that appeared to contradict other findings, said Paul Ottinger, research fisheries biologist at the U.S. Geological Survey's Leetown Science Center in Kearneysville, WV. Mycobacteriosis appeared in significant amounts in the bay's rockfish, or striped bass, population about a decade ago. Researchers know that the Chesapeake, where most rockfish spawn, also breeds the bacterium and is the epicenter of the disease. Yet they don't know how or why it appeared, whether it will spread to other species or if the infection it causes is always fatal. The epidemic could carry profound implications for rockfish, which fuel a $300 million industry in Maryland and Virginia. But because the bacteria kill slowly, effects on the stock are only now emerging.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/05/11/AR2006051101984.html

27. *May 11, Dow Jones* — **U.S. might consider statewide farm quarantines for bird flu.** In the event of a situation with multiple outbreaks of the H5N1 strain of bird flu in poultry flocks, the U.S. Department of Agriculture (USDA) could decide to enact a statewide quarantine on poultry farms, a USDA official said at a U.S. Senate Agriculture Committee hearing Thursday, May 11. Ron DeHaven, administrator of USDA's Animal and Plant Health Inspection Service, said a large−scale quarantine would restrict the movement of birds. Also, "equipment, feed trucks, anything that would be coming on and off a poultry premise ... would not be allowed to move" unless a permit was issued "and then only after proper cleaning and disinfection." A statewide quarantine would be an "extreme" situation, DeHaven said. The more likely scenario would be a targeted quarantine of a single premise.
Source: http://www.cattlenetwork.com/content.asp?contentid=36404

[Return to top]

Food Sector

28. *May 12, Associated Press* — **Bill would track where recalled meat goes.** Food distributors would have to provide the state of California with a list of stores and restaurants that received deliveries of recalled meat or poultry under a bill sent to Governor Arnold Schwarzenegger on Thursday, May 11. Local public health officials want the information so they can publicize potential outbreaks. They have been thwarted, however, by an agreement by the state Department of Health Services to keep secret any information about recalls that comes from the U.S. Department of Agriculture (USDA). Current USDA policy does not allow the release of meat distribution lists during a recall, and states have to agree to follow that policy to get information about recalls. California agreed to that requirement in a 2002 memorandum of understanding with the USDA that prohibits the state from giving meat distribution information to the public. The bill, given final approval by the state Senate on a 23−13 vote, attempts to get around the federal restrictions by requiring poultry and meat suppliers to directly inform state health officials when they recall products. The state could then tell county health officials and the public.
Source: http://www.contracostatimes.com/mld/cctimes/news/local/states/california/14561903.htm

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

29. *May 14, New York Times* — **Avian flu wanes in Asian nations it first hit hard.** Even as it crops up in the far corners of Europe and Africa, the H5N1 strain of bird flu that raised fears of a human pandemic has been largely snuffed out in the parts of Southeast Asia where it claimed

its first and most numerous victims. "In Thailand and Vietnam, we've had the most fabulous success stories," said David Nabarro, chief pandemic flu coordinator for the United Nations. Vietnam, which has had almost half of the human cases of H5N1 flu in the world, has not seen a single case in humans or a single outbreak in poultry this year. Thailand, the second−hardest−hit nation until Indonesia recently passed it, has not had a human case in nearly a year or one in poultry in six months. Encouraging signs have also come from China, though they are harder to interpret.
Source: http://www.nytimes.com/2006/05/14/world/asia/14flu.html?_r=1&oref=slogin

30. *May 14, Xinhua (China)* — **Indonesia local tests show five positive on bird flu.** Five Indonesian people from a family related by blood were positively infected by the H5N1 avian influenza virus, a health ministry official said Saturday, May 13. Director General of Disease Control of the ministry, I Nyoman Kandun said that the five from Indonesia's North Sumatra province had had contacts with fowls and pigs. He said that their blood samples had been sent to the World Health Organization's (WHO) affiliated laboratory in Hong Kong. The five are 29 year−old woman, two men 19 years old and 35, whom have died since at the end of last month, and two others men 25 years old and 35 years old man, whom survive, according to the director. The director said that tree others people from the family were suspected of having the virus, including a 40 year−old woman and a 10 year−old boy, both of which have died, and a 35 year−old man who survived.
Source: http://feed.insnews.org/v−cgi/feeds.cgi?feedid=150&story_id=1832399

31. *May 11, KENS 5 (TX)* — **Doctors puzzled over infection surfacing in South Texas.** Doctors are trying to find out what is causing a mysterious infection that's surfaced in South Texas. Morgellons disease is not yet known to be fatal. "These people will have like beads of sweat but it's black and tarry," said Ginger Savely, a nurse practioner in Austin who treats a majority of these patients. Patients get lesions that never heal. "Sometimes little black specks that come out of the lesions and sometimes little fibers," said Stephanie Bailey, Morgellons patient. So far more than 100 cases of Morgellons disease have been reported in South Texas. So far, pathologists have failed to find any infection in the fibers pulled from lesions. Randy Wymore, a researcher at the Morgellons Research Foundation at Oklahoma State University's Center for Health Sciences, examines the fibers, scabs and other samples from Morgellon's patients to try and find the disease's cause. No one knows how Morgellans is contracted, but it does not appear to be contagious. The states with the highest number of cases are Texas, California and Florida.
Mogellons disease information: http://www.morgellons.org/
Source: http://www.mysanantonio.com/news/metro/stories/MYSA051106.morgellans.KENS.32030524.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

32. *May 12, Associated Press* — **FEMA goes high−tech for storm preparedness.** The Federal Emergency Management Agency (FEMA) has a live video network to allow officials in Washington, DC, to assess disasters and has equipped trucks with global positioning system devices so the agency can see when supplies are delivered to stricken areas, officials said Thursday, May 11. To better prepare for this year's hurricane season, FEMA has also stockpiled equipment for floods and started a partnership with the Coast Guard to use its boats when responding to some emergencies.
Source: http://abcnews.go.com/Politics/wireStory?id=1952893

33. *May 12, Loveland FYI (CO)* — **Disaster drill at nuclear site puts local response agencies to the test.** Two Idaho companies specializing in nuclear fuel provided Weld County, CO's, former nuclear power plant with a tornado exercise Wednesday, May 10. The Department of Energy and its Idaho contractors have supplied mock−disaster training every two years for the Independent Spent Fuel Storage Installation since it began housing used nuclear fuel in 1991. The exercise called upon response from the Milliken and Johnstown police departments, Platteville/Gilcrest Fire Protection District, Weld County dispatch, Office of Emergency Management and paramedics, Milliken Fire Department and Fort St. Vrain Security, among others. Emergency officials reported minor trouble communicating over radio channels but said they were pleased with their work to secure the facility, aid the victims and find and secure the radioactive tools.
Source: http://www.lovelandfyi.com/region−story.asp?ID=5144

34. *May 12, Gleaner News (KY)* — **Severe weather drill highlights the importance of ham radios.** In a severe weather drill Thursday, May 11, negative temperatures, freezing rain and sleet turned Henderson, KY, and its surrounding counties into a veritable ice kingdom. The objective of this drill: For emergency responders within the seven counties of the Green River Area Development District to share information regarding disaster preparedness. The event comprised three hospitals and seven counties −− Henderson, Union, Webster, Daviess, Hancock, McLean and Ohio −− and each county had to communicate with each other. Some problems involved written communications between the agencies involved. But one positive result −− emergency personnel rediscovered the benefits of ham radios as a form of communication when trying to reach other counties.
Source: http://www.courierpress.com/ecp/gleaner_news/article/0,1626,ECP_4476_4692575,00.html

35. *May 12, Beaumont Enterprise (TX)* — **Regionalism key to Southeast Texas hurricane plan.** With three weeks left until the start of hurricane season, Southeast Texas leaders met Wednesday, May 10, to settle details of response plans. Jefferson County Judge Carl Griffith will serve as regional coordinator for at least Jefferson, Orange and Hardin counties. "Regionalism is the key factor right now," said Orange County Judge Carl Thibodeaux. Planning has included provisions for greater fuel availability, new destinations for buses carrying Southeast Texas evacuees and moves toward more pre−disaster contracts. Griffith said state contracts should ensure greater fuel availability along evacuation routes if a hurricane threatens again. Gas stations normally keep tanks at about 25 percent capacity. In the future, designated refueling stations that contract with the state will fill to 75 percent capacity 120 hours before tropical storm−force winds are expected, Griffith said. A map of the designated

refueling stations should be finalized in about two weeks.
Source: http://www.southeasttexaslive.com/site/news.cfm?newsid=16627213&BRD=2287&PAG=461&dept_id=512589&rfi=6

[Return to top]

Information Technology and Telecommunications Sector

36. *May 11, FrSIRT* — **Apple QuickTime multiple remote buffer and integer overflow vulnerabilities.** Multiple vulnerabilities were identified within Apple QuickTime, which could be exploited by remote attackers to take complete control of an affected system. Analysis: Integers overflow error when processing malformed JPEG images could be exploited by remote attackers to execute arbitrary commands via a malicious Webpage. Remote attackers could successfully execute arbitrary commands that may initiate integer overflow errors from malformed QuickTime movies obtained from a malicious Website.
Affected products: Apple QuickTime versions prior to 7.1 (Mac OS X and Windows).
Solution: Upgrade to Apple QuickTime version 7.1:
http://www.apple.com/support/downloads/quicktime71.html
Source: http://www.frsirt.com/english/advisories/2006/1778

37. *May 11, FrSIRT* — **Apple Mac OS X multiple remote and client−side code execution vulnerabilities.** Apple has released security updates to address thirty−one vulnerabilities identified in Mac OS X. These flaws could be exploited by attackers to execute arbitrary commands, bypass security restrictions, disclose sensitive information, or cause a denial−of−service.
Affected products: Apple Mac OS X version 10.4.6 and prior; Apple Mac OS X Server version 10.4.6 and prior; Apple Mac OS X version 10.3.9 and prior; Apple Mac OS X Server version 10.3.9 and prior. Solution: Security Update 2006−003 for Mac OS X 10.4.6 Client (PPC):
http://www.apple.com/support/downloads/securityupdate2006003 macosx1046clientppc.html
Security Update 2006−003 for Mac OS X 10.4.6 Client (Intel):
http://www.apple.com/support/downloads/securityupdate2006003 macosx1046clientintel.html
Security Update 2006−003 for Mac OS X 10.3.9 Client:
http://www.apple.com/support/downloads/securityupdate2006003 1039client.html
Security Update 2006−003 for Mac OS X 10.4.6 Server:
http://www.apple.com/support/downloads/securityupdate2006003 1046server.html
Security Update 2006−003 for Mac OS X 10.3.9 Server:
http://www.apple.com/support/downloads/securityupdate2006003 1039server.html
Source: http://www.frsirt.com/english/advisories/2006/1779

38. *May 11, Security Focus* — **Linux kernel IPv6 flowlable denial−of−service vulnerability.** Linux kernel is prone to a local denial−of−service vulnerability. Analysis: A flaw in the IPv6 flowlabel code allowed a local user to cause a denial−of−service. Local attackers can exploit this vulnerability to corrupt kernel memory or free non−allocated memory. Successful exploitation will crash the kernel, effectively denying service to legitimate users.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/15729/info
Solution: For more information and fixes: http://www.securityfocus.com/bid/15729/references
Source: http://www.securityfocus.com/bid/15729/discuss

39. *May 11, SecuriTeam* — **Holes in the Linux random number generator: paper.** A new paper was recently released which describes holes in Linux's random number generator, as well as a clear description of the Linux /dev/random. The Linux random number generator is part of the kernel of all Linux distributions and is based on generating randomness from entropy of operating system events. The output of this generator is used for almost every security protocol, including TLS/SSL key generation, choosing TCP sequence numbers, and file system and e−mail encryption. Although the generator is part of an open source project, its source code is poorly documented, and patched with hundreds of code patches. This paper presents a description of the underlying algorithms and exposes several security vulnerabilities.
Analysis of the Linux Random Number Generator paper:
http://www.gutterman.net/publications/GuttermanPinkasReinman 2006.pdf
Source: http://www.securiteam.com/unixfocus/5RP0E0AIKK.html

40. *May 10, CRN* — **Exchange SP1 patch conflicts with Blackberry, GoodLink.** One of the three security bulletins Microsoft released last week for Exchange could cause problems for Blackberry and GoodLink users. Microsoft released a patch for Exchange 2003 SP1 called MS06−019 that includes a configuration change that eliminates a default privilege granting any users with "full mailbox access" permission to "Send As" the mailbox owner. Microsoft claims customers asked that "Send As" permission be separated from the "Full Mailbox Access" permission to deter e−mail spoofing. The change to the Exchange configuration may cause issues for Blackberry Enterprise Server and Good Technology's GoodLink Wireless Messaging, Microsoft security experts said during its monthly security call Wednesday, May 10. According to the Microsoft knowledgebase, users cannot send e−mail messages from a mobile device or from a shared mailbox in Exchange 2000 and Exchange Server 2003.
Source: http://www.crn.com/sections/software/software.jhtml?articleI d=187201975

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 38566 (−−−), 445 (microsoft−ds), 12198 (−−−), 25 (smtp), 41170 (−−−), 6588 (AnalogX), 49200 (−−−), 32459 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.